UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/802,370	03/17/2004	Charles J. Lathram	190250-1890	3796

38823 7590 04/29/2008

THOMAS, KAYDEN, HORSTEMEYER & RISLEY, LLP/
AT&T Delaware Intellectual Property, Inc.
600 GALLERIA PARKWAY, S.E.
SUITE 1500
ATLANTA, GA 30339-5994

EXAMINER	
FLEISCHER, MARK A	

ART UNIT	PAPER NUMBER
4143	

MAIL DATE	DELIVERY MODE
04/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/802,370	LATHRAM ET AL.	
	Examiner	Art Unit	
	MARK A. FLEISCHER	4143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 April 2005 and 17 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☒ Claim(s) *14,16 and 17* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 March 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Status of Claims

1. This action is in reply to the Application filed on 17 March 2004.
2. Claims 1–22 are currently pending and have been examined.

Priority

3. Applicant's claim for the benefit of a prior-filed provisional application 60/508629 under 35 U.S.C. 119(e) is hereby acknowledged.

Drawings

4. The drawings are objected to under 37 CFR 1.83(a) because they fail to show details as described in paragraph [0043] of the specification. The text states that "Within … system 100…each Governance group 210-270…" where the elements 210-270 are not indicated within the framework denoted by system 100. Also, servers 141-145 are not shown but clearly referenced in [0033] of the specification. Any structural detail that is essential for a proper understanding of the disclosed invention should be shown in the drawing. MPEP § 608.02(d). Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended.
5. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: 400, 510, 1310, 1500, 1810, 1855, 1860, 1870 and 1880. Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance

with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

6. The disclosure is objected to because of the following informalities: there is no mention of reference characters 400, 510, 1310, 1500, 1810, 1855, 1860, 1870 and 1880 in the description as noted in the objection to the drawings above. Appropriate correction is required.

Claim Objections

7. Claim 14 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. The claim provides for the inclusion of *significant issues,* issues that are *new* and *that occur across multiple operational units*. The set of *significant issues* already encompasses these issues and thus the claim does not further limit the parent claim.
8. Claim 16 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or

amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. The claim either expands the definition of "collective knowledge" by using the term "includes", or delineates elements already incorporated under the rubric "collective knowledge", hence does not further limit the parent claim.

9. Claim 17 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. The claim either expands the definition of "collective knowledge" by using the term "includes", or delineates elements already incorporated under the rubric "collective knowledge", hence does not further limit the parent claim.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

11. Claims 5–9 and 11–22 are rejected under 35 U.S.C. 102(b) as being anticipated by Williams (*Information Security Governance*).

Claim 5:

Williams, as shown, describes and/or discloses the following limitations.

- *individually summarizing data from a plurality of governance databases located on a business network of a business enterprise* (Williams, in at least page 66 states: "The security function has the means and ability to detect, record, analyse, report and act upon security incidents when they do occur, while minimising the probability of occurrence by applying intrusion testing and active monitoring" (emphasis added)

where 'report' and 'active monitoring' corresponds to *individually summarizing data*. Also, on page 69, box 4: "Security processes are coordinated with the overall organization security function and reporting is linked to business objectives" (emphasis added) where the 'reporting' is associated with the 'overall organization', hence *from a plurality of governance databases located on…);*

- *reviewing the data at an enterprise level to identify one or more significant issues to the business enterprise* (Williams, in at least page 65, col. 1, top, states: "Conduct periodic reviews and tests" (emphasis added) which is done, *ipso facto to identify one or more…issues*. Also, on page 64, Williams also describes this limitation: "Establish monitoring measures to detect and ensure correction of security breaches, so that all actual and suspected breaches are promptly identified, investigated and acted upon, and to ensure ongoing compliance with policy, standards and minimum acceptable security practices" (emphasis added) where 'monitoring measures…' corresponds to *reviewing the data,* 'suspected breaches are … identified' corresponds to *to identify* and where the 'breaches' are a *significant issue to the business enterprise.*);
- *determining a plan, at the enterprise level, to address the significant issue across the business enterprise* (Williams, in at least page 70, box 5 states: "Security requirements are clearly defined, optimised and included in a verified security plan. Functions are integrated with applications at the design stage and end users are increasingly accountable for managing security. IT security reporting provides early warning of changing and emerging risk, using automated active monitoring approaches for critical systems. Incidents are promptly addressed with formalised incident response procedures supported by automated tools." (emphasis added) where 'clearly defined' and 'security plan' and 'formalised incident…procedures' corresponds to *determining a plan* and 'changing and emerging risk' corresponds to *the significant issue* where all these elements are associated with an 'enterprise'

(see, *e.g.,* page 60 and on for frequent references to the enterprise), hence corresponds to *at the enterprise level.); and*

- *communicating the plan to each operational unit within the business enterprise* (Williams, in at least page 64, col. 2 states: "**Take Management Level Action** • Write the security policy, with business input (Policy Development); • Ensure that individual roles, responsibilities and authority are clearly communicated and understood by all." (emphasis added) where 'the security policy' corresponds to *the plan*, 'ensure…individual roles…' corresponds *to each operational unit within…* and 'clearly communicated' corresponds with *communicating the plan.*).

Claim 6:

Williams describes and/or discloses the limitations of claim 5 as shown above. Williams further describes and/or discloses the following limitations.

- *the plan involves developing business controls for addressing the significant issue* (Williams, in at least page 64, col. 2 states: "Develop a security and control framework that consists of standards, measures, practices, and procedures […]" (emphasis added) where 'Develop…control framework' corresponds to *developing business controls* and on page 70, box 5 refers to "adequate mitigating controls are promptly communicated and implemented." (emphasis added) where 'mitigating controls' corresponds to controls that mitigate some detrimental effects associated with *the significant issue,* hence corresponds to *for addressing the significant…*).

Claim 7:

Williams describes and/or discloses the limitations of claim 5 as shown above. Williams further describes and/or discloses the following limitations.

- *implementing the plan within each operational unit of the business enterprise* (Williams, in at least page 62, col. 2 states: "Implementing the solution on a timely basis, then maintaining it" (emphasis added) where 'implementing the solution' corresponds to *implementing the plan.* On page 63, col. 1, bottom, Williams further

states: "[F]or information security to be properly addressed, greater involvement of boards of directors, executive management and business process owners is required. For information security to be properly implemented, skilled resources such as information systems auditors, security professionals and technology providers need to be utilized. All interested parties should be involved in the process […]" (emphasis added) where the emphasized text corresponds to *each operational unit* so that the plan can be 'properly implemented' hence corresponds to *implementing…*).

Claim 8:

Williams describes and/or discloses the limitations of claim 7 as shown above. Williams further describes and/or discloses the following limitations.

- *tracking the progress of the plan in addressing the significant issue within each operational unit* (Williams, in at least page 65, col. 2 states: "Measurement process with feedback on progress made" (emphasis added) and on page 66, col. 1: "Conduct information security audits based on a clear process and accountabilities with management tracking closure of recommendations." (emphasis added) where 'management tracking…' and 'progress made' corresponds to *tracking the progress of…*and pertains to *the significant issue* since such security audits are used to identify security breaches which are a species of *the significant issue.*).

Claim 9:

Williams describes and/or discloses the limitations of claim 5 as shown above. Williams further describes and/or discloses the following limitations.

- *analyzing, at the enterprise level, each significant issue to ascertain a respective cause of the significant issue* (Williams, in at least page 70, box 5 states: "Intrusion testing, root cause analysis of security incidents and proactive identification of risk is the basis for continuous improvements. Security processes and technologies integrated organization wide." (emphasis added) where 'root cause analysis'

corresponds to *analyzing …to ascertain a respective cause…* and 'organization wide' corresponds to *at the enterprise level.* Finally, note that 'security incidents' corresponds to *each significant issue*...which is further delineated in box 5 of the reference.).

Claim 11:

Williams describes and/or discloses the limitations of claim 5 as shown above. Williams further describes and/or discloses the following limitations.

- *electronically accessing each governance database containing governance data for operational units of the enterprise* (Williams, in at least page 61, col. 2 states: "In this context, "valuable assets" are the data or information recorded on, processed by, stored in, shared by, transmitted or retrieved from an electronic medium." (emphasis added) where 'valuable assets are …' corresponds to *governance data for operational units of…*and 'retrieved' corresponds to *accessing* and 'electronic medium' corresponds to *electronically accessing.* Note also that on page 63, col. 1, Williams states: "Responsibility for governing and managing the improvement of security has consequently too often been limited to operational and technical managers. However, for information security to be properly addressed, greater involvement of boards of directors, executive management and business process owners is required." (emphasis added) where the emphasized text collectively corresponds to *operational units of the enterprise.*)*; and*
- *utilizing a person familiar with a particular governance database to complete a template summarizing the governance data contained in the particular governance database for the operational units* (Williams, in at least page 66, col. 1 states: "Develop clear policies and detailed guidelines, supported by a repetitive and assertive communications plan" (emphasis added) where 'develop…detailed guidelines' corresponds to *complete a template summarizing…*Note that Williams on page 66, col. 2 states: "Management and staff have a common understanding of

security requirements, vulnerabilities and threats, and understand and accept their own security responsibilities." (emphasis added) where 'management and staff' and 'understanding' together correspond to *utilizing a person familiar with…*and further implies that the 'detailed guidelines' corresponds to *governance data for the operational units* since 'staff' and 'responsibilities' together imply a plurality of such *units*.).

Claim 12:

Williams/Holmstrom describe and/or disclose the limitations of claim 11 as shown above. Williams further describes and/or discloses the following limitations.

- *the template includes areas for providing details concerning the significant issue and the operational units affected by the significant issue* (Williams, in at least page 66, col. 1 states: "Develop clear policies and detailed guidelines, supported by a repetitive and assertive communications plan" (emphasis added) where 'detailed guidelines' corresponds to *the template includes areas for providing details…*See also the rejection of claim 11 above with respect to the *operational units affected by*. Also, 'clear policies' corresponds to rules associated with important matters that affect various enterprise entities, hence corresponds to *affected by the significant issue*.)

Claim 13:

Williams describes and/or discloses the limitations of claim 5 as shown above. Williams further describes and/or discloses the following limitations.

- *the method is performed at periodic intervals* (Williams, in at least page 64 states "Take Management Level Action" and on page 65: "Conduct periodic reviews and tests").

Claim 14:

Williams describes and/or discloses the limitations of claim 5 as shown above. Williams further describes and/or discloses the following limitations.

- *significant issues include issues that are new and issues that occur across multiple operational units* (Williams, in at least page 63, col. 1 states: "This means that there are new or re-focused risk areas that could have a significant impact upon critical business operations such as: [ ] Growing potential for misuse and abuse of information systems affecting privacy and ethical values" (emphasis added) where 'new' and 'significant impact' correspond to *significant issues …that are new*, 'abuse of information systems' are *significant issues …that occur across multiple operational units* since issues affecting information systems can have enterprise-wide effects.).

Claim 15:

Williams describes and/or discloses the limitations of claim 5 as shown above. Williams further describes and/or discloses the following limitations.

- *utilizing collective knowledge within the business enterprise to identify the one or more significant issues* (Williams, in at least page 66, col. 1 states: "Develop what-if scenarios on information security and risk, leveraging the knowledge of the specialists" (emphasis added) where 'develop…' corresponds to *to identify …significant issues,* and 'leveraging the knowledge …' corresponds to *utilizing collective knowledge within the business enterprise…*).

Claim 16:

Williams describes and/or discloses the limitations of claim 15 as shown above. Williams further describes and/or discloses the following limitations.

- *the collective knowledge within the business enterprise includes an understanding of current business practices of the operational units* (Williams, in at least page 64, col. 2 states: "Ensure that individual roles, responsibilities and authority are clearly communicated and understood by all." (emphasis added) where 'understood by all' corresponds to *the collective knowledge within the business enterprise…*On page 62, col. 2, Williams states: "Awareness, Training and Education—Creating awareness of the need to protect information, providing training in the skills needed to operate

information systems securely, and offering education in security measures and practices." (emphasis added) where 'creating awareness' also corresponds to *collective knowledge* and 'providing training…' in conjunction with 'measures and practices' and 'understood by all' corresponds to *understanding of current business practices of the operational units.*).

Claim 17:

Williams describes and/or discloses the limitations of claim 15 as shown above. Williams further describes and/or discloses the following limitations.

- *the collective knowledge within the business enterprise includes an understanding of recent legal matters concerning the enterprise* (Williams, in at least page 63, col. 2 states: "As news of break-ins and losses related to hackers, computer viruses and other Internet-based threats grows more frequent, enterprise stakeholders are becoming concerned about the risks, regulatory requirements and investments associated with information security." (emphasis added) where 'news of', 'regulatory requirements' and 'enterprise stakeholders' corresponds to *recent legal matters concerning the enterprise*. Also, 'becoming concerned' corresponds to *an understanding of* as they pertain to 'regulatory requirements', hence *recent legal matters.*).

Claim 18:

Williams describes and/or discloses the limitations of claim 5 as shown above. Williams further describes and/or discloses the following limitations.

- *reviewing the data at the enterprise level to identify one or more issues that occur within a domain of a single operational unit* (See the rejection of the correspondent limitation in claim 5. Further note that Williams delineates these and similar method steps to involve both "Board Level Action" and "Management Level Action" (see page 64) hence corresponds to *data at the enterprise level* further to *identify one …issue[] within… a single operational unit* where 'board level' review encompasses *a single*

…unit to wit on page 63, col. 1 Williams states: "However, for information security to be properly addressed, greater involvement of boards of directors, executive management and business process owners is required. For information security to be properly implemented, skilled resources such as information systems auditors, security professionals and technology providers need to be utilized. All interested parties should be involved in the process – but the buck stops at Board level. Governance is all about senior directors understanding the risks and the opportunities and gaining positive assurance that these are being properly and continuously managed." (emphasis added) where the emphasized text corresponds to various *operational units* for which issues are identified.)*;*

- *determining a strategy, at the single operational unit level, to address the one or more issues that occur within the domain of the single operational unit* (See the rejection of the correspondent limitation in claim 5 and the rejection of the preceding limitation.)*;*
- *communicating the strategy to each operational unit within the enterprise* (See the rejection of the correspondent limitation in claim 5 and the rejection of the preceding limitation.)*; and*
- *monitoring the progress of the strategy, at an enterprise level* (Williams, in at least page 65, col.2 states: "Require that the head of security report progress and issues to the audit committee or direct to the Board itself" (emphasis added) where 'report progress' corresponds to *monitoring the progress of the strategy* and 'to the Board itself' corresponds to *at an enterprise level.*).

Claim 19:

Williams, as shown, describes and/or discloses the following limitations.

- *forming an integrated governance team to identify problematic issues in designated governance areas across a business enterprise, the integrated governance team comprising members having knowledge of each of the designated governance areas*

and of operational units within the enterprise (Williams, in at least page 65, col. 2 states: "• Establish ownership for security and continuity with enterprise managers; • Create an audit committee that clearly understands its role in information security and how it will work with management and auditors" (emphasis added) where 'establish ownership' in conjunction with 'create an audit committee' corresponds to *forming an integrated governance team to identify problematic issues…*since an audit committee is but one example of a group that seeks to *identify* problems. As this is done at the "board level" (see page 65) it pertains to *issues…across a business enterprise*. Moreover, on page 65 col. 1 Williams states: "Properly prioritised and distributed effort to areas with greatest impact and business benefit" (emphasis added) and on page 60, col. 2 states: "This has recently been issued by the IT Governance Institute, a body established on a global basis to establish thought leadership and to promulgate best practices in all areas of the governance of IT." (emphasis added) where 'areas of the governance' corresponds to *designated governance areas.*);

- *compiling data from a plurality of databases that contain information regarding the governance areas for a plurality of the operational units in the enterprise* (Williams, page 70, box 5 states: "Information on new threats and vulnerabilities is systematically collected and analysed, and adequate mitigating controls are promptly communicated and implemented." (emphasis added) where 'new threats…' corresponds to *information regarding governance areas* and 'systematically collected' corresponds to *compiling data from*. Also note that on page 61, col. 2, Williams refers to "data or information recorded on …an electronic medium" hence corresponds to such data as *from a plurality of databases.*);
- *integrating together data from the plurality of databases to form a comprehensive summary of governance information for the enterprise* (See the rejection of the previous limitation. Also note that in conjunction with the previous rejection, Williams on page 65 states: Ensure that internal and external auditors agree with the audit

committee and management how information security should be covered in the audit; • Require that the head of security report progress and issues to the audit committee or direct to the Board itself;" and on page 66 states: "Develop clear policies and detailed guidelines, supported by a repetitive and assertive communications plan" (emphasis added) where reference to 'audit' corresponds to *integrating together data from…*and further, 'report' and 'detailed guidelines' corresponds to *a comprehensive summary of governance…*);

- *analyzing, as a team, the comprehensive summary to identify one or more significant issues within the governance areas for the enterprise* (Williams, in at least page 64, col.2, states: "Analyse risks, or identify industry practice for due care, analyse vulnerabilities" (emphasis added) where 'analyse…' corresponds to *analyzing, as a team* since this analysis is done within the scope of "Management Level Action" and where such is *a team*. Also, 'identify industry practice' and 'vulnerabilities' corresponds to a *identify [a] significant issue[ ] within…*);
- *utilizing collective knowledge of the integrated governance team to uncover the fundamental cause of the respective significant issue* (Williams, in at least page 70, box 5 states: "Information on new threats and vulnerabilities is systematically collected and analysed, and adequate mitigating controls are promptly communicated and implemented. Intrusion testing, root cause analysis of security incidents and proactive identification of risk is the basis for continuous improvements. Security processes and technologies integrated organization wide." (emphasis added) where 'information on …' and 'integrated organization wide' corresponds to *utilizing collective knowledge of the integrated …* and 'root cause analysis' corresponds to *to uncover the fundamental cause…* and where 'threats and vulnerabilities' corresponds to species of a *respective significant issue.*); *and*
- *forming, as a team, a comprehensive plan to address the fundamental cause of the respective significant issue across the enterprise* (Williams, in at least page 65, col. 2

states: "Create an audit committee that clearly understands its role in information security and how it will work with management and auditors; […] • Develop crisis management practices, involving executive management and the board of directors from pre-agreed thresholds onwards." (emphasis added) where in respect of the rejection of the previous limitation, 'create an audit committee' corresponds to *forming, as a team,* 'develop crisis management practices' corresponds to *a comprehensive plan to address…*Note that it is **inherent** for a group that engages in 'crisis management' *to address the fundamental cause* of problems and issues confronting said group.).

Claim 20:

Williams, as shown, describes and/or discloses the limitations of claim 19 as shown above. Williams further describes and/or discloses the following limitations.

- *the compiling step is performed by particular members familiar with the information contained in the databases* (Williams, in at least page 70, box 5 states: "• IT security is a joint responsibility of business and IT management and integrated with corporate business objectives. […] Information on new threats and vulnerabilities is systematically collected and analysed, and adequate mitigating controls are promptly communicated and implemented." (emphasis added) where the 'joint responsibility of …' and 'systematically collected…' corresponds to *the compiling step is performed by particular members familiar* since IT management is *familiar with …information …in…databases* by virtue of their function.).

Claim 21:

Williams, as shown, describes and/or discloses the limitations of claim 19 as shown above. Williams further describes and/or discloses the following limitations.

- *communicating the plan to each of the operational units in the enterprise* (Williams, in at least page 64, col. 2 states: "**Take Management Level Action** • Write the security policy, with business input (Policy Development); • Ensure that individual roles,

responsibilities and authority are clearly communicated and understood by all." (emphasis added) where 'the security policy' corresponds to *the plan*, 'ensure…individual roles…' corresponds *to each operational unit within…* and 'clearly communicated' corresponds with *communicating the plan.*).

Claim 22:

Williams, as shown, describes and/or discloses the limitations of claim 19 as shown above. Williams further describes and/or discloses the following limitations.

- *the comprehensive plan involves developing business controls for addressing the respective significant issue* (Williams, in at least page 60, col. 2 states: "These practices were intended to improve standards of corporate behaviour, strengthen business controls, and ensure accountability whilst retaining the essential spirit of the enterprise." (emphasis added) where 'these practices' corresponds to *the comprehensive plan* and 'strengthen business controls' corresponds to *developing business controls*. On page 62, col. 2, Williams further asserts that one of six major activities regarding security, a significant issue, is "Developing a security and control framework that consists of standards, measures, practices and procedures" (emphasis added) where 'developing' a 'control framework' also corresponds to *developing business controls* and 'framework' also corresponds to *the comprehensive plan.*).

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been

obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

    a) Determining the scope and contents of the prior art.
    b) Ascertaining the differences between the prior art and the claims at issue.
    c) Resolving the level of ordinary skill in the pertinent art.
    d) Considering objective evidence present in the application indicating obviousness or nonobviousness.

14. Claims 1–4, and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Williams (*Information Security Governance*) in view of Holmstrom (*The State of U.S. Corporate Governance: …*).

Claim 1:

Williams does not specifically describe and/or disclose the following limitation, but Holmstrom, as shown, does.

- *a plurality of governance sources monitoring respective governance areas within a business enterprise* (Holmstrom, in at least page 21 refers to "the audit committee" and on page 24 refers to the "compensations committees…");

Holmstrom does not specifically describe and/or disclose the following limitation(s), but Williams, as shown, does.

- *a plurality of governance databases, each database maintained by a respective governance source* (Williams, in at least page 62 states: "Data and information are disclosed only to those who have a right to know (confidentiality); • Data and information are protected against unauthorised modification (integrity); […] The relative priority and significance of availability, confidentiality and integrity vary according to the data within the information system and the business context in which the data are used." (emphasis added) where 'only to those…' corresponds to *a*

respective governance source and 'unauthorised modification' and 'business context…' corresponds to a *database* that is *maintained* since it is 'used', and *ipso facto maintained.*);

- *at least one or more communication networks interconnecting the plurality of governance databases* (Williams, in at least page 62 repeatedly refers to communications networks as in "The networked economy…" and on page 63 "other Internet-based threats…". Furthermore, Williams clearly refers to the infrastructure that supports such communications on page 66: "Strengthen all security and critical server and communications platforms;" and on page 62: "The objective of information security is: 'protecting the interests of those relying on information, and the systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality and integrity.'" (emphasis added) where 'relying on information…' corresponds to *the plurality of governance databases.*); *and*
- *an integrated governance team reviewing data within the plurality of governance databases to identify significant issues for the enterprise in the governance areas* (Williams, in at least page 60 states: "Even though it is delegated to management, the Board is ultimately responsible for this system of internal control'." (emphasis added) and on page 70: "IT security is a joint responsibility of business and IT management and integrated with corporate business objectives." (emphasis added) where the 'Board' corresponds to *an integrated governance team,* and 'system of internal control' corresponds to *governance areas* since, as indicated, the 'board' is ultimately responsible for governance. 'IT management' also corresponds to *an integrated governance team* and 'integrated with …' corresponds to *governance team reviewing data* since IT management must, *ipso facto,* review data to make informed decisions. Also, on page 64 it is stated: "Both the Board and executive management need to take appropriate actions to achieve their security governance objectives. **Take Board Level Action** • Become informed about information security;"

(emphasis added) where 'become informed' also corresponds to *governance team reviewing data*. Note also that on page 62, Williams further states: "The relative priority and significance of availability, confidentiality and integrity vary according to the data within the information system and the business context in which the data are used." (emphasis added) where 'significance of…', as indicated, is antecedent to a set of *significant issues…*).

Holmstrom describes a number of governance areas in a typical enterprise. Williams further elaborates on methods for instituting effective information security governance in the typical enterprise. Both of these references recite a number of elements that are important to corporate governance in the information age and document, to one degree or another, actions and decisions and methods that corporate management teams and boards of directors frequently confront in their efforts to effectively manage and control an enterprise. Therefore, it would have been obvious to one with ordinary skill in the art at the time of the invention to combine the teachings of Holmstrom and Williams because together they delineate important elements for effective corporate governance.

Claim 2:

Williams/Holmstrom describe and/or disclose the limitations of claim 1, as shown above. Williams, as shown, further describes and/or discloses the following limitations.

- *the integrated governance team further determines a plan, at an enterprise level, to address the significant issue across the enterprise* (Williams, in at least page 65-6 states: "At the Executive Management Level […] Establish clear, pragmatic enterprise and technology continuity programmes, continually tested and kept up to date" (emphasis added) where 'executive management…' corresponds to *the integrated governance team,* 'Establish…programmes' corresponds to *determines a plan* and where 'pragmatic enterprise…technology continuity' corresponds to *the significant issue across the enterprise* since technology continuity is an example of a *significant issue*.).

Claim 3:

Williams/Holmstrom describe and/or disclose the limitations of claim 1, as shown above. Williams, as shown, further describes and/or discloses the following limitations.

- *a database of the integrated governance team for storing a summary of governance information from the plurality of governance databases* (Williams, in at least page 70, box 5 states: "IT security is a joint responsibility of business and IT management […] Information on new threats and vulnerabilities is systematically collected and analysed, and adequate mitigating controls are promptly communicated and implemented." (emphasis added) where 'IT management' corresponds to *the integrated governance team,* 'information on…' corresponds to *a summary of governance information* and 'systematically collected…' corresponds to *a database …for storing…*since the information is stored on a database in an environment associated with an 'optimized' IT infrastructure.).

Claims 4 and 10:

Although claims 4 and 10 are worded and/or structured slightly differently, they have the same scope and so are addressed together. Williams/Holmstrom describe and/or disclose the limitations of claims 1 as shown above and Williams describes and/or discloses the limitations of

claim 5, as shown in the §102(b) rejections above. Williams, as shown, further describes and/or discloses the following limitations.

- *the plurality of governance sources include at least one from the group of*
  - *an audit department,*
  - *a security department,*
  - *an ethics department,*
  - *a business controls department, and*
  - *a compliance department* (**Examiner's Note**: the foregoing limitations corresponds to a Markush grouping and thus this rejection will address some, but not necessarily all, of the elements of the group. Williams, in at least page 67 states: "There is senior management support to ensure that employees perform their duties in an ethical and secure manner" (emphasis added) where 'senior management support' corresponds to a *governance source* that involve 'ethical' and 'secur[ity]' concerns. Also, note that on page 60 Williams refers to "Audit Committees".).

Examiner's Note: The Examiner has pointed out particular references contained in the prior art of record within the body of this action for the convenience of the Applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply. Applicant, in preparing the response, should consider fully the entire reference as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Conclusion

Any inquiry of a general nature or relating to the status of this application or concerning this communication or earlier communications from the Examiner should be directed to **Dr. Mark A. Fleischer** whose telephone number is **571.270.3925.** The Examiner can normally be reached on Monday-Friday, 9:30am-5:00pm. If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, **James A. Reagan** whose telephone number is **571.272.6710** may be contacted.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://portal.uspto.gov/external/portal/pair <http://pair-direct.uspto.gov >. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at **866.217.9197** (toll-free).

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

Washington, D.C. 20231

or faxed to **571-273-8300**.

Hand delivered responses should be brought to the **United States Patent and Trademark Office Customer Service Window**:

Randolph Building

401 Dulany Street

Alexandria, VA 22314.

Mark A. Fleischer, Ph.D.
/Mark A Fleischer/
Examiner, Art Unit 4143
24 April 2008
/James A. Reagan/
Supervisory Patent Examiner, Art Unit 4143